HSPD-12:
How will you be affected ?

Roslin K. Hicks
MSFC HSPD-12 Implementation Manager
November 17, 2006

AGENDA

□ What is HSPD-12?

□ What does it really mean?

□ What does the MSFC HSPD-12 Implementation Project Include?

□ What are the NASA & OMB Milestones?

□ Will there be badging changes?

□ What are the new Investigation Requirements?

□ What will the Investigations cost our Center?

□ Will Computers or Applications Change?

□ What else will change with Applications?

□ What are the benefits of HSPD-12?

□ How is Security Being Improved?

□ What will be Achieved?

□ How will we work?

□ Who is leading the HSPD-12 Implementation at MSFC?

What is HSPD-12?

❑ The White House issues Homeland Security Presidential Directive 12 (HSPD-12) on August 27, 2004, following the OMB and GAO reports on inadequate network security in government Information Technology (IT) operations

❑ HSPD-12's primary objective is the development and deployment of a Federal Government-wide common and reliable identification verification system that will be interoperative among all government agencies, and serve as the basis for reciprocity among those agencies.

What does it really mean?

The Directive mandates:

- ❑ Requires more rigorous background checks and proof of an individual's identity
- ❑ More secure physical and logical access to federal facilities and systems
- ❑ Background investigations for all civil servants, contractors, and offsite or remote-only IT users
- ❑ Requires a standard badge format (Smart Card) throughout the federal government for civil servants and contractors
- ❑ Two-factor authentication to IT systems, applications, desktops, laptops, and servers utilizing a standard Smart Card

Additional activities included in NASA's implementation of HSPD-12:

- ❑ Integration of IT user and resource accounts into the NASA Account Management System (NAMS)

What does the MSFC HSPD-12 Implementation Project Include?

1. Support of the National Agency Checks and Inquiries
2. Supporting the work efforts for Personal Identity Verification compliant badge

   (Smart Card) issuance
3. Migration to Smart Authentication for desktops and servers
4. The integration of IT resource accounts into the NAMS environment
5. Enable two-factor authentication on applications

What are the NASA & OMB Milestones?

Oct 27, 2006	• Issue required identity credentials (badges) for all NEW Civil Servant and Contractor employees, compliant with FIPS 201 PIV Standard • Part 1 (Standard identity vetting process for badges and NACI background checks) • Part 2 (Smart Cards, i.e., enable two-factor authentication) • Implement a Final Acceptance Review (FAR) Clause for the Standard in applicable contracts
Apr 30, 2007	• Utilize PIV II validated Smart Cards to access desktop computers
Sept 30, 2007	• Two-factor authentication enable all applications that are categorized HIGH per FIPS 199
Oct 27, 2007	• Complete re-issuance of required identity credentials for all CURRENT civil servant and contractor employees, compliant with Parts 1 and 2 of the Standard
Sept 30, 2008	• Two-factor authentication enable all applications that are categorized MODERATE per FIPS 199
Oct 27, 2008	• For individuals who have been with NASA over 15 years, NACI investigations can be delayed based on risk, but all must be done by this date
Sept 30, 2010	• Two-factor authentication enable all applications that are categorized LOW per FIPS 199 that the risk warrants

***NASA HSPD-12 Milestones, shows the NASA dates interlaced with the OMB HSPD-12 Milestones. NASA milestone dates*

Will there be badging changes?

All individuals will receive a Personal Identification Verification (PIV) compliant badge.

There are two types of PIV badges: PIV-1 and PIV-2.

- **PIV-1** is the “One NASA” badge. All NASA Civil Servants and Contractors (currently being issued) have a PIV-1 badge.

- **PIV-2** is the new Smart Card Badge. The new Smart Card badge is in essence a PIV-1 badge with the addition of Public Key Infrastructure (PKI), biometrics, keys, and certificates that will authenticate users and allow access to IT resources and area locations. PIV-2 badges (to be issued throughout 2007) will replace PIV-1 badges.

What are the new Investigation requirements?

- ❑ Civil servants and contractors must have a National Agency Check and Inquiries (NACI) investigation and their fingerprints on file in order to be eligible to receive a PIV badge.
- ❑ Most MSFC Current NASA civil servants already have NACIs
- ❑ New contractor individuals are currently getting NACI and PIV-1 badges
- ❑ Many current contractor individuals do not have a NACI or PIV badges. Security is working with contractor personnel to schedule NACI and PIV badging

What will Investigations cost our Center ?

- □ **Civil Servant Risk Determination NASA Form 1722**

- □ **Contractor Risk Determination MSFC Form 4482**

	Low	Moderate	High
Civil Servant	**NACI (97)** **10 years**	**MBI (525)** **7 years**	**BI (2825)** **5 years**
Contractor	**NACI (97)** Initiated on Standard Form 85 **10 years**	**NACI w/credit (107)** Initiated on Standard Form 85P **10 years**	**BI (2825)** Initiated on Standard Form 85P **5 years**

***Approximate cost of investigation in parenthesis*

*- Re-investigation requirement in **red***

Will Computers or Applications Change?

Desktops/Laptops/Servers:

□ Installation of Smart Card Readers and software will take place on most computers.

Applications:

□ Some applications will be transitioned to two-factor authentication. Two-factor authentication is generally defined as something you have (Smart Card) and something you know (password or PIN), which is used to authenticate you to the application.

□ Applications that will require two-factor authentication will be divided into three categories (high, moderate, and low), based on National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199 specifications. Each category will be converted over different timelines of the project.

□ Not all applications will require two-factor authentication. In general, if an application today doesn’t require a username/password combination to access the application, then it will not be changed.

What else will change with Applications?

To request/change/modify an application account you will be using a new system called the NASA Account Management Systems (NAMS). This system will manage system account requests or changes for logical access to IT resources (systems, applications, servers, etc.)

- ❑ It provides consistent and accurate account management processes across the Agency
- ❑ Ensures that people requesting accounts on IT resources have a valid identity
- ❑ Ensures that the account requests are reviewed, and then approved or denied
- ❑ Ensures rapid removal of access to IT resources when individuals leave the Agency
- ❑ Enforces Agency policies and processes

What are the benefits of HSPD-12?

❑ Helps protect NASA’s investments from intentional or unintentional harm.

❑ Minimizes the number of passwords to remember.

❑ Reduces the risk of identity theft by increasing protection of personal privacy.

❑ Interoperability across the Agency for access to facilities and information systems.

How is Security Being Improved?

- ❑ A credential is issued only to an individual whose true identity has been ascertained by the issuer.
- ❑ Only an individual with a background investigation on record is issued a credential.
- ❑ An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid federal or state government issued picture ID.
- ❑ Fraudulent identity source documents are not accepted as genuine and unaltered.
- ❑ A person suspected or known to the government as being a terrorist is not issued a credential.
- ❑ No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued.
- ❑ No credential is issued unless requested by proper authority.
- ❑ A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked
- ❑ A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential
- ❑ An issued credential is not modified, duplicated, or forged

What Will Be Achieved?

- ❑ Automate Agency processes
- ❑ Digitally identify employees and contractors
- ❑ Digitally monitor physical and logical access
- ❑ Reduce the numbers of credentials needed
- ❑ Reduce passwords needed
- ❑ Inventory what we have versus what we need, with senior level commitment, based on architecture and cost models
- ❑ Integration of smart cards, electronic readers, back end identity management databases, and intelligent middleware and workflow to form a fully accredited PIV system
- ❑ Manage rights and privileges without issuing new cards when rights and privileges changes, unless intentional
- ❑ Depend on others both internally and externally to have validated their respective users and vouch for their access, based on process control

How Will We Work?

- ❑ Strong verification of each user's identity before being issued a Smart Card
- ❑ PIV card used to provide employee access throughout the day both physically and logically
- ❑ Goal is to have a converged secure environment (*standard card, issued based on sound criteria for verifying identity, resistant to fraud, rapidly authenticated electronically, issued by an organization whose reliability has been certified and accredited*)

Who is leading the HSPD-12 Implementation at MSFC?

MSC HSPD-12 Steering Committee

Organization	MSFC Point of Contact
Office of the Director	DE01 / Robin Henderson
Center Operations (AS)	AS01/Ann McNair
Human Capital (HS)	HS01/ Tereasa Washington
Office of the CIO (IS)	IS01/Jonathan Pettus
Office of Procurement	PS01/ Steve Beale

MSFC HSPD-12 Core Team

Organization	MSFC Point of Contact
MSFC HSPD-12 IM	EI52/Roslin Hicks
Procurement (PS)	PS12 / T Jerry Williams, Cynthia Hollingsworth, Pam White
Protective Services (AS)	AS50 / Rip, Nabors, Becky Hopson
Human Capital (HS)	HS50 / Dana Blaine & Deborah Longeddy
Office of the CIO (IS)	IS30 / Steve Deutschendorf, Marcellus Graham

MSFC HSPD-12 Extended Team

Project/Activity	MSFC Point of Contact
NASA Integrated Services Environment Project (NISE)	IS30 / Steve Deutschendorf
Identity Management System (IDMS)	AS50/ Becky Hopson IS50/ Sharon Ing
NASA Account Management System (NAMS)	IS30 / Marcellus Graham
Cyber Identity Management System (CIMS)	IS30 / Steve Deutschendorf
Active Directory	IS40 / Linda Porter
E-Authentication	IS50 / Sharon Ing
Common Badging and Access Control System (CBACS)	AS50 / Becky Hopson (Common Badging) AS50 / Justin Jackson (Access Control) AS50 / Debbie Swafford (Personnel Investigations)
Public Key Infrastructure (PKI)	AS50/ Justin Jackson IS40 / Linda Porter
InsideNASA	IS30 / Steve Deutschendorf
NASA Applications Review – Working Group (NAR-WG)	IS30 / Steve Deutschendorf
Desktop Integration (SMART CARD – ODIN AND NON ODIN)	IS40 / Burt Bright
MSFC Account Authorization Official (AAO)	IS30 / Marcellus Graham

MSFC HSPD-12 Extended Center Team

Name	Org		Name	Org
Justin Jackson	AS01		John Pea	MP01
Terry Minor	CS01		Willie Love	OS01
Anne Vinson	DA, DD, DE		Dwight Clark	PS01
Keith Niehuss	ED01		Dane Garver	QD01
Lou Nosenzo	HS01		Bill Vaughn	RS01
Lisa Hall	HS01		Sharon Chunn	RS01
Steve Deutschendorf	IS01		Anthony Goodeill	VP01
Marcellus Graham	ISO1		Steve Spearman	VP01
Elizabeth Sudderth	IS40		Paige Vaughn	VP01
Tom Oliver	IS60			
Robert Robb	JP01			
Jim McGroary	LS01			

***This team formed as result of request from IS01 / generally managed by Steve Deutschendorf*

Back – Up Charts

Project Defining Events

2002

- ❑ **Office of Security and Program Protection (OSPP) created the Smart Card Project and the Identity Management System (IDMS) for the development of a common credential token for granting access to NASA's physical and logical resources**
- ❑ **GSA Smart Card Task Order awarded**

1/2004

- ❑ **OSPP and OCIO directed that implementation of common badging and access control systems would precede the use of Smart Cards**

7/2004

- ❑ **President signed Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors**
  - Mandated a common identification standard for federal employees and contractors
  - Unprecedented opportunity for Federal Agencies to put into place a trusted identity and authentication management that will both enhance their own security and interoperate across Federal government

Project Defining Events (Cont.)

2/2005

- **NIST released initial Federal Information Processing Standard (FIPS) 201**
  - PIV-I – Control objectives for identity proofing and chain of trust
  - PIV-II – Technical interoperability and security requirements
  - Per OMB M-05-24, phase in issuance and use of identity credentials meeting the standard no later than October 27, 2007

2005-2006

- **Federal standards and specifications continued to be revised:**
  - NIST 800-73-1, March 2006 NIST 800-85A, April 2006
  - FIPS PUB 201-1, March 2006 NIST 800-85B, July 2006
  - NIST 800-76, February 2006 NIST 800-96, Sept. 2006

HSPD 12 High Level Requirements

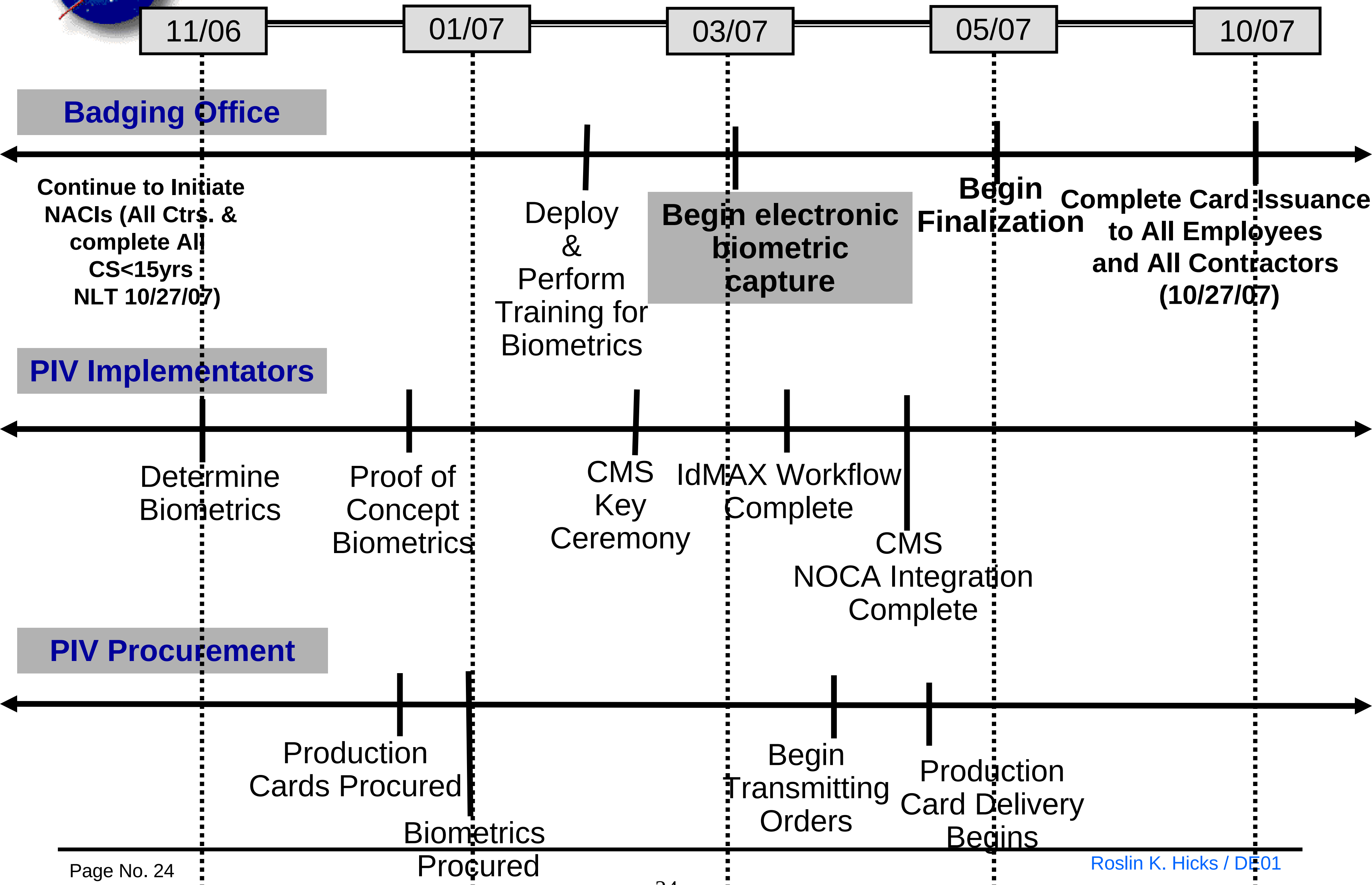
- ❑ **Proofing**
  - An individual’s true identity has been ascertained by the issuer
  - A background investigation is on record prior to issuing a credential
  - Two identity source documents, at least one of which is a valid federal or state government issued picture ID.
  - Fraudulent identity source documents are not accepted as genuine and unaltered.
  - A person suspected or known to the government as being a terrorist is not issued a credential.
  - No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued
- ❑ **Accredited Providers**
  - No credential is issued unless requested by proper authority.
  - A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential
- ❑ **Resistance to Tampering/Fraud/Counterfeiting**
  - A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked
  - An issued credential is not modified, duplicated, or forged

NASA PIV High Level Requirements

The NASA PIV System shall:

- Comply with FIPS 201 requirements for applicant enrollment, card production, and card issuance for Federal employees
- Create and store new identities for new NASA employees, contractors and partners
- Track information related to identity proofing documents, fingerprints, and background checks
- Issue a PIV-II compliant Smart Card badge that contains a PKI identity certificate and capability for optional PIV certificates
- Manage the issuance lifecycle for PIV-II compliant Smart Cards
- Flow information appropriately through interconnected NASA systems (AD, CIMS, CBACS)
- Produce NASA PIV cards for which CBACS is able to enable physical access control
- Provide NASA data via automated interface to Office or Personnel Management (OPM) and/or Federal Bureau of Investigation (FBI) in acceptable format
- Support commercial bulk printing of NASA PIV cards as well as Face-to-Face NASA PIV printing
- Within all subsystem components, meet NIST 800-53 HIGH controls

PIV Critical Events



11/06 01/07 03/07 05/07 10/07

Badging Office

Continue to Initiate NACIs (All Ctrs. & complete All CS<15yrs NLT 10/27/07)

Deploy & Perform Training for Biometrics

Begin electronic biometric capture

Begin Finalization

Complete Card Issuance to All Employees and All Contractors (10/27/07)

PIV Implementators

Determine Biometrics

Proof of Concept Biometrics

CMS Key Ceremony

IdMAX Workflow Complete

CMS NOCA Integration Complete

PIV Procurement

Production Cards Procured

Biometrics Procured

Begin Transmitting Orders

Production Card Delivery Begins

High, Moderate and Low Definitions

The *potential impact* is HIGH if -

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The *potential impact* is MODERATE if -

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

The *potential impact* is LOW if -

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

For full amplification of the High, Moderate and Low classifications please obtain a copy of the reference document titled: FIPS PUB-199: (Standards for Security Categorization of Federal Information and Information Systems).

What Problems Does CBACS Solve ?

- ❑ Provides a central authoritative repository of all NASA identity information
- ❑ Replaces outdated badging systems to one standard, centrally managed suite of software and hardware products
- ❑ Allows NASA Civil Servants to travel or to be temporarily assigned to other NASA locations using the same badge
- ❑ Leverages automated workflow for the creation of Agency business rules and processes (e.g., badge requests, badge approval, access approval, and terminations) using NASA Integrated Services Environment (NISE)
- ❑ Allows NASA to deploy Federally-approved Smart Card technology in conjunction with identity management (HSPD 12 and FIPS-201)
- ❑ Provides two-factor authentication for logical access to NASA resources
- ❑ Validates current Agency identity data
- ❑ Changes the identity verification and validation paradigm from visual to electronic

How Will It Work? (A Few Good Questions)

Question 1: FIPS 201 requires that remote unlocking of a smartcard or remote re-issuance of certificates requires biometric authentication. Can users unlock their own cards after specified numbers of bad tries?

FIPS 201 states that a PIN may be reset if the card is locked due to exceeding number of bad PIN tries. FIPS 201 requires that the biometrics on the card be checked to ensure the card belongs to the cardholder. Updates to the card are not allowed without proper access control. Therefore, providing the user an ability to unlock the card without a biometric fingerprint match will not meet FIPS 201 requirements.

Question 2: Do the PIV Sponsor, Registrar, PIV Card Approval and the PIV issuer have to be all different people, or can one person have multiple roles?

FIPS 201 states that "the PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person." Thus, the standard states that separation of duties must occur, but it does not explicitly state how separation of duties must be implemented.

How Will It Work? (continued)

Question 3: If there are employees and contractors working on contracts or services that support a tenant agency, can a PIV be issued by the host agency on whose property they work or does the PIV have to be issued by the agency that they are employed by?

FIPS 201 suggests that the sponsorship for card issuance should originate with the employing agency. There is nothing to prohibit one agency from providing issuance services to another agency in accordance with interagency MOA/MOU.

Question 4: What will the card look like?

Various possible configurations of the card topology are included in the standard. Each card will contain a required set of items (e.g., a printed picture of the cardholder, name, expiration date, etc.) However, the appearance of the cards will vary a bit among agencies as each agency will decide which of the optional fields (e.g., signature, agency seal, issue date, etc.) they choose to use—or even define their own, within the flexibility provided by the new standard.

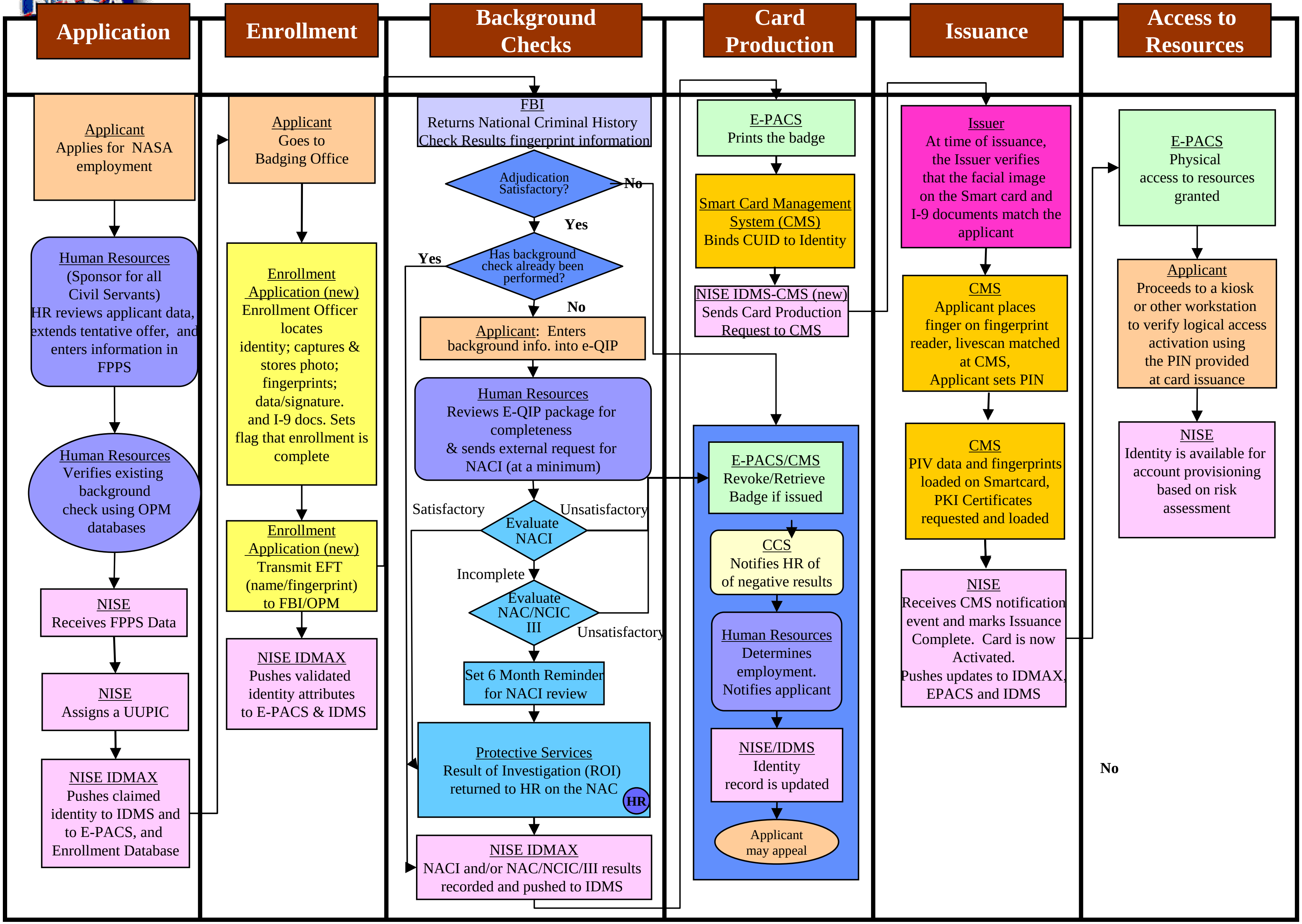
How Will It Work? (continued)

Question 5: What information is required to be stored on the card?

Only a minimal amount of information is required to be electronically stored on the card. The PIV Card must contain only the following data:

1. Personal Identification Number (PIN)—this data is used to authenticate the cardholder to the card--in the same way a PIN is used with an ATM card. The PIN never leaves the card, and it cannot be read from the card.
2. A Cardholder Unique Identifier (CHUID)—this number uniquely identifies the individual within the PIV system.
3. Two fingerprint biometrics that are PIN protected.
4. One asymmetric cryptographic key pair used to authenticate the card to the PIV system.

The standard does not require any other personal information such as the cardholder's SSN, address, or phone number to be stored on the card. Release of biometric information and use of the private key can take place only AFTER the cardholder provides the correct PIN number. Only the Cardholder Unique Identifier is required by the standard to be available through the contactless interface.



Application

Applicant
Applies for NASA employment

Human Resources
(Sponsor for all Civil Servants)
HR reviews applicant data, extends tentative offer, and enters information in FPPS

Human Resources
Verifies existing background check using OPM databases

NISE
Receives FPPS Data

NISE
Assigns a UUPIC

NISE IDMAX
Pushes claimed identity to IDMS and to E-PACS, and Enrollment Database

Enrollment

Applicant
Goes to Badging Office

Enrollment Application (new)
Enrollment Officer locates identity; captures & stores photo; fingerprints; data/signature. and I-9 docs. Sets flag that enrollment is complete

Enrollment Application (new)
Transmit EFT (name/fingerprint) to FBI/OPM

NISE IDMAX
Pushes validated identity attributes to E-PACS & IDMS

Background Checks

FBI
Returns National Criminal History Check Results fingerprint information

Adjudication Satisfactory?

No

Yes

Has background check already been performed?

Yes

No

Applicant: Enters background info. into e-QIP

Human Resources
Reviews E-QIP package for completeness & sends external request for NACI (at a minimum)

Satisfactory

Unsatisfactory

Evaluate NACI

Incomplete

Evaluate NAC/NCIC III

Unsatisfactory

Set 6 Month Reminder for NACI review

Protective Services
Result of Investigation (ROI) returned to HR on the NAC

HR

NISE IDMAX
NACI and/or NAC/NCIC/III results recorded and pushed to IDMS

Card Production

E-PACS
Prints the badge

Smart Card Management System (CMS)
Binds CUID to Identity

NISE IDMS-CMS (new)
Sends Card Production Request to CMS

E-PACS/CMS
Revoke/Retrieve Badge if issued

CCS
Notifies HR of of negative results

Human Resources
Determines employment. Notifies applicant

NISE/IDMS
Identity record is updated

Applicant may appeal

Issuance

Issuer
At time of issuance, the Issuer verifies that the facial image on the Smart card and I-9 documents match the applicant

CMS
Applicant places finger on fingerprint reader, livescan matched at CMS, Applicant sets PIN

CMS
PIV data and fingerprints loaded on Smartcard, PKI Certificates requested and loaded

NISE
Receives CMS notification event and marks Issuance Complete. Card is now Activated. Pushes updates to IDMAX, EPACS and IDMS

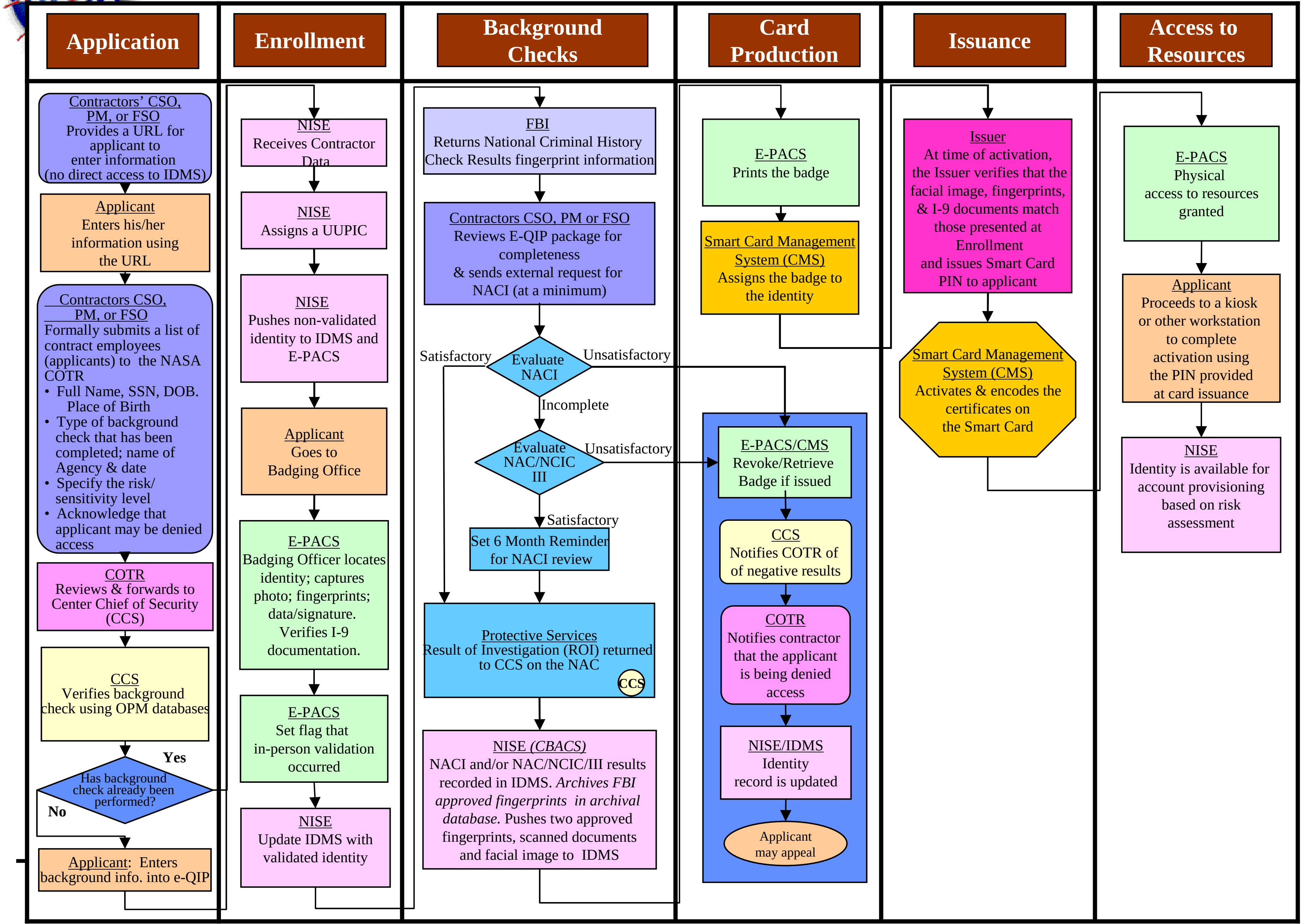
Access to Resources

E-PACS
Physical access to resources granted

Applicant
Proceeds to a kiosk or other workstation to verify logical access activation using the PIN provided at card issuance

NISE
Identity is available for account provisioning based on risk assessment

No



Application

Contractors' CSO, PM, or FSO
Provides a URL for applicant to enter information (no direct access to IDMS)

Applicant
Enters his/her information using the URL

Contractors CSO, PM, or FSO
Formally submits a list of contract employees (applicants) to the NASA COTR

- Full Name, SSN, DOB. Place of Birth
- Type of background check that has been completed; name of Agency & date
- Specify the risk/ sensitivity level
- Acknowledge that applicant may be denied access

COTR
Reviews & forwards to Center Chief of Security (CCS)

CCS
Verifies background check using OPM databases

Has background check already been performed?

Yes

No

Applicant: Enters background info. into e-QIP

Enrollment

NISE
Receives Contractor Data

NISE
Assigns a UUPIC

NISE
Pushes non-validated identity to IDMS and E-PACS

Applicant
Goes to Badging Office

E-PACS
Badging Officer locates identity; captures photo; fingerprints; data/signature. Verifies I-9 documentation.

E-PACS
Set flag that in-person validation occurred

NISE
Update IDMS with validated identity

Background Checks

FBI
Returns National Criminal History Check Results fingerprint information

Contractors CSO, PM or FSO
Reviews E-QIP package for completeness & sends external request for NACI (at a minimum)

Evaluate NACI

Satisfactory

Unsatisfactory

Incomplete

Evaluate NAC/NCIC III

Unsatisfactory

Satisfactory

Set 6 Month Reminder for NACI review

Protective Services
Result of Investigation (ROI) returned to CCS on the NAC

CCS

NISE *(CBACS)*
NACI and/or NAC/NCIC/III results recorded in IDMS. *Archives FBI approved fingerprints in archival database.* Pushes two approved fingerprints, scanned documents and facial image to IDMS

Card Production

E-PACS
Prints the badge

Smart Card Management System (CMS)
Assigns the badge to the identity

E-PACS/CMS
Revoke/Retrieve Badge if issued

CCS
Notifies COTR of of negative results

COTR
Notifies contractor that the applicant is being denied access

NISE/IDMS
Identity record is updated

Applicant may appeal

Issuance

Issuer
At time of activation, the Issuer verifies that the facial image, fingerprints, & I-9 documents match those presented at Enrollment and issues Smart Card PIN to applicant

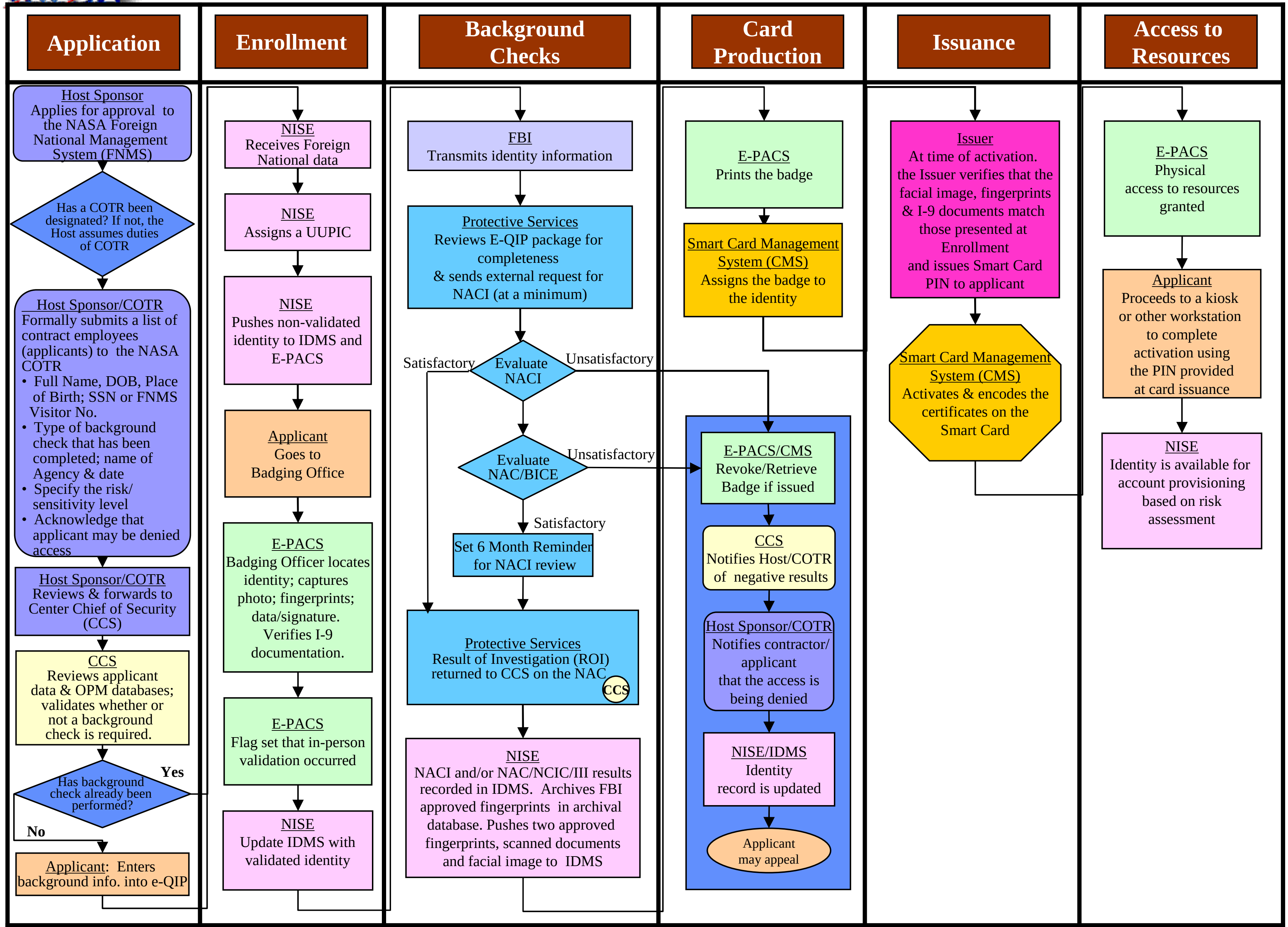
Smart Card Management System (CMS)
Activates & encodes the certificates on the Smart Card

Access to Resources

E-PACS
Physical access to resources granted

Applicant
Proceeds to a kiosk or other workstation to complete activation using the PIN provided at card issuance

NISE
Identity is available for account provisioning based on risk assessment



Application

Host Sponsor
Applies for approval to the NASA Foreign National Management System (FNMS)

Has a COTR been designated? If not, the Host assumes duties of COTR

Host Sponsor/COTR
Formally submits a list of contract employees (applicants) to the NASA COTR
- Full Name, DOB, Place of Birth; SSN or FNMS Visitor No.
- Type of background check that has been completed; name of Agency & date
- Specify the risk/ sensitivity level
- Acknowledge that applicant may be denied access

Host Sponsor/COTR
Reviews & forwards to Center Chief of Security (CCS)

CCS
Reviews applicant data & OPM databases; validates whether or not a background check is required.

Has background check already been performed?

Yes

No

Applicant: Enters background info. into e-QIP

Enrollment

NISE
Receives Foreign National data

NISE
Assigns a UUPIC

NISE
Pushes non-validated identity to IDMS and E-PACS

Applicant
Goes to Badging Office

E-PACS
Badging Officer locates identity; captures photo; fingerprints; data/signature. Verifies I-9 documentation.

E-PACS
Flag set that in-person validation occurred

NISE
Update IDMS with validated identity

Background Checks

FBI
Transmits identity information

Protective Services
Reviews E-QIP package for completeness & sends external request for NACI (at a minimum)

Evaluate NACI

Satisfactory

Unsatisfactory

Evaluate NAC/BICE

Unsatisfactory

Satisfactory

Set 6 Month Reminder for NACI review

Protective Services
Result of Investigation (ROI) returned to CCS on the NAC

CCS

NISE
NACI and/or NAC/NCIC/III results recorded in IDMS. Archives FBI approved fingerprints in archival database. Pushes two approved fingerprints, scanned documents and facial image to IDMS

Card Production

E-PACS
Prints the badge

Smart Card Management System (CMS)
Assigns the badge to the identity

E-PACS/CMS
Revoke/Retrieve Badge if issued

CCS
Notifies Host/COTR of negative results

Host Sponsor/COTR
Notifies contractor/ applicant that the access is being denied

NISE/IDMS
Identity record is updated

Applicant may appeal

Issuance

Issuer
At time of activation. the Issuer verifies that the facial image, fingerprints & I-9 documents match those presented at Enrollment and issues Smart Card PIN to applicant

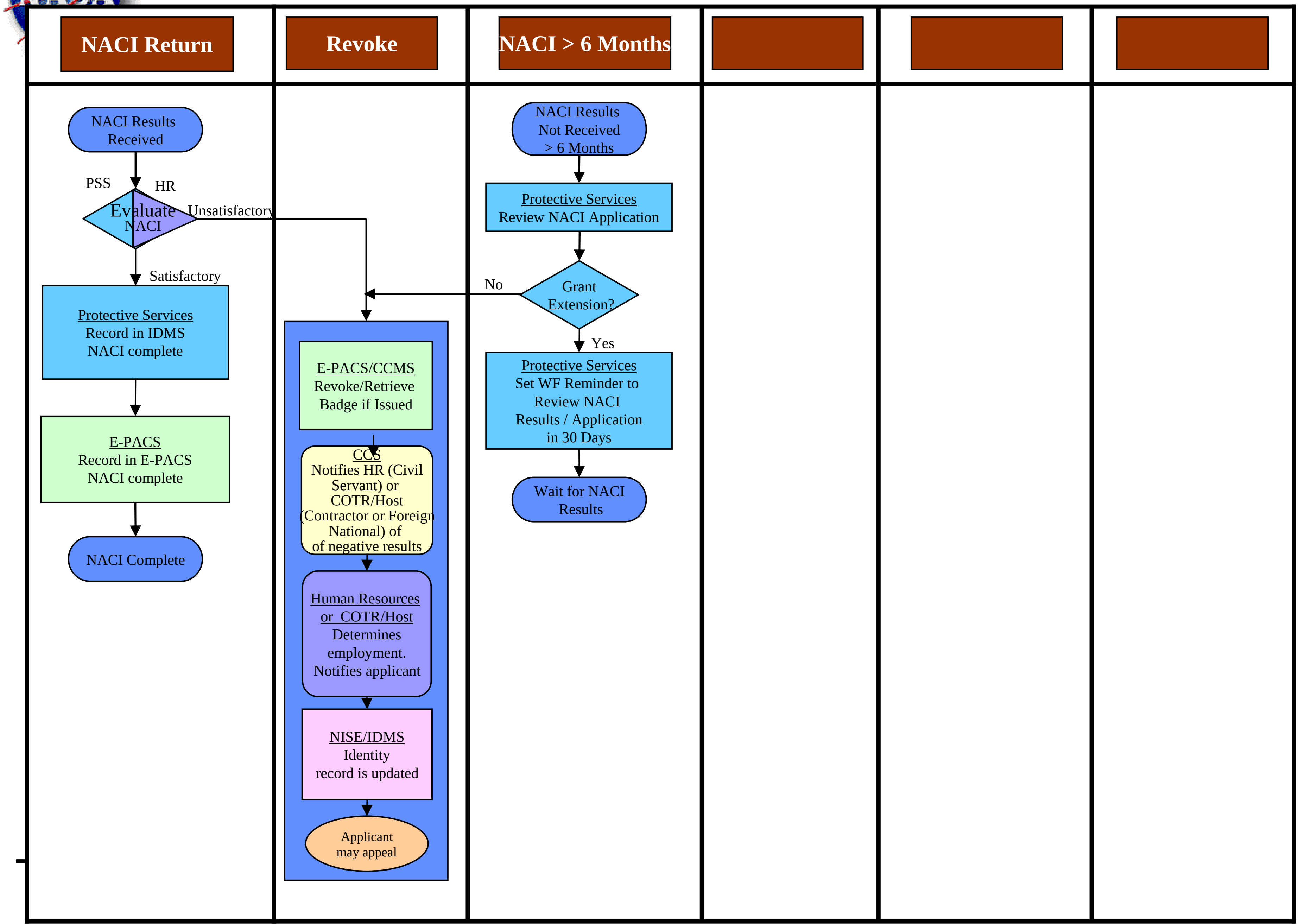
Smart Card Management System (CMS)
Activates & encodes the certificates on the Smart Card

Access to Resources

E-PACS
Physical access to resources granted

Applicant
Proceeds to a kiosk or other workstation to complete activation using the PIN provided at card issuance

NISE
Identity is available for account provisioning based on risk assessment



NACI Return

NACI Results Received

PSS

HR

Evaluate NACI

Unsatisfactory

Satisfactory

Protective Services
Record in IDMS
NACI complete

E-PACS
Record in E-PACS
NACI complete

NACI Complete

Revoke

E-PACS/CCMS
Revoke/Retrieve
Badge if Issued

CCS
Notifies HR (Civil Servant) or COTR/Host (Contractor or Foreign National) of of negative results

Human Resources or COTR/Host
Determines employment.
Notifies applicant

NISE/IDMS
Identity record is updated

Applicant may appeal

NACI > 6 Months

NACI Results Not Received > 6 Months

Protective Services
Review NACI Application

Grant Extension?

No

Yes

Protective Services
Set WF Reminder to Review NACI Results / Application in 30 Days

Wait for NACI Results

MSFC HSPD-12 Website

Under development